(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 March 2001 (29.03.2001)

PCT

(10) International Publication Number
WO 01/22406 A1

(51) International Patent Classification[7]: G11B 5/02, H04N 5/91

(21) International Application Number: PCT/SE00/01835

(22) International Filing Date:
20 September 2000 (20.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9903461-3 24 September 1999 (24.09.1999) SE

(71) Applicant *(for all designated States except US)*: **PROTEGO INFORMATION AB** [SE/SE]; Ideon, S-223 70 Lund (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **DÖMSTEDT, Bo** [SE/SE]; Teknikergatan 5, S-215 68 Malmö (SE). **STENFELDT, Mats** [SE/SE]; Filippavägen 26, S-222 41 Lund (SE).

(74) Agents: **BERGMAN, Kerstin** et al.; Albihns Patentbyrå Malmö AB, P.O. Box 4289, S-203 14 Malmö (SE).

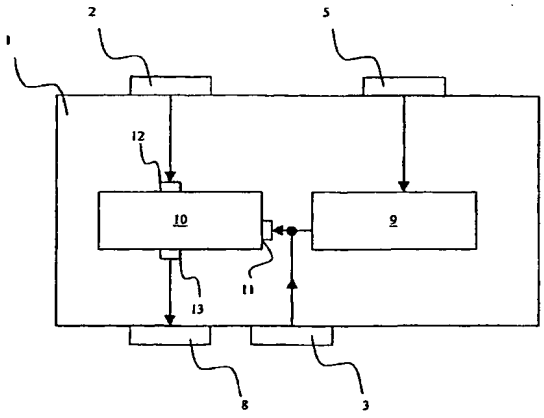
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR IDENTIFICATION MARKING OF A DATA STREAM



(57) Abstract: A method and an apparatus for implementing an identification code together with the data of a data stream, and to actively introduce a disturbance signal into the data stream, obscuring the presence of the identification code. In a preferred embodiment the disturbance signal is true random noise at a level below the cognitive threshold of a viewer or listener of the material that is represented by the data stream. Since the noise has true random behaviour, subtraction of one copy from another will not lead to any decrease in noise level. Hence, such a comparison will not lead to the unconvering of the indentity codes. The inventive apparatus and method is preferably used for recording audio or video material on digital recording media, including optical means such as DVD and CD as well as magnetic tape recording media, but is also useable for analog recordings. The invention is particularly suitable for marking video data streams transmitted to a video-on-demand user.

WO 01/22406 A1

METHOD AND APPARATUS FOR IDENTIFICATION MARKING OF A DATA STREAM

Technical field

The present invention relates to a method and apparatus for marking and preparing streams of data such as video or audio data, for the purpose of tracing the source of unauthorised copying and distribution.

Background

A few years ago most commercial distributions of movies or music recordings were on analog media, such as VHS, Compact Cassette or LP records. With the rapid evolution of electronics during the recent years, most of the volume that was distributed on analog media is being replaced by digital media, and in a lot of areas the digital media is already dominating.

It is a well-known fact that illegal copying of analog media is a severe problem to the music and film industry. However, an illegal copy of an LP recording onto a tape cassette, for instance, will not have the same quality as the original recording, due to addition of noise in the copying process. With the introduction of digital distribution media this problem will be more severe, as the copies will be identical to the original and of perfect quality. Therefore the noise problem disappears, making it possible to mass distribute a copy which may be obtained in the end of a chain of sequential illegal copies.

Consequently, illegal copies pose a serious threat to distributors of digital media within many different areas. The music industry has been stunned by the potentials of the MP3-format, allowing music recordings to be distributed over the Internet without generating any profit for the record companies. Another business area having big problems with illegal copies is the computer program manufacturers. This concerns both programs intended for office use and games developed for personal computers.

One way of in inhibiting that certain information is detected and recreated by someone else than the intended recipient, is to use some encryption technique. Advances in Cryptology, Proceedings of Crypto 82, by Chauns, Rivest and Sherman, Plenum Press ISBN 0-306-41366-3, Randomized Encryption Techniques p. 145-163, teaches several ways of using random bit sequence generators for encrypting information. Two problems with encryption, however, is firstly that pirates historically have found ways to crack encryption, in effect, obtaining the key without paying for it, and secondly, for the case of digital media, that once a single

legitimate copy of some content has been decrypted, the pirate is free to make unlimited copies of the decrypted copy.

Trying to attack the actual copying is indeed a very difficult task. Hence, a lot of effort has been made to come up with ideas to inhibit the distribution of illegal copies. A way of achieving this is to provide each copy with an identification code so that each purchaser, or group of purchasers, receives a unique copy. However, it is important that the identification code is transported to any new copies made from the purchase copy, in order for the source of the illegal copying to be traceable. The company, or the people, who intend to sell illegally copied will of course try to obscure the source of the original material. Any identification code printed or hidden on e.g. the sleeve of a Compact Disc (CD) may clearly be removed by issuing new material replacing the old encoded material. Consequently, the only place where the identification code may be securely placed is inside the recorded data itself.

A state of the art procedure for marking digital media with an identification code is thus to select a predetermined portion, in time and/or space, of the recorded material and to insert a code signal on the selected portion. For video recording e.g. the luminance of a certain pixel at a certain point in time is raised whereas the luminance for another pixel next to the first pixel is lowered, leaving the average luminance unaltered. Endless ways of introducing different sequences of altered information that are inconceivable by the end-user, i.e. the viewer or listener of the material, can be thought of. Since this code is inserted into the data of the material, direct copying of the material, e.g. music or film, will also include the code. US patent 5,613,004, which is hereby incorporated by reference, discloses an apparatus and a method for encoding and decoding additional information into a stream of digitised samples in an integral manner. The information is enclosed using special keys. The information is contained in the samples, not prepended or appended to the sample stream. The proposed solution thus combines two techniques, steganography – obscuring information that is otherwise in plain sight, and cryptography – scrambling information that must be sent over unsecured means, such that only the intended recipient may successfully unscramble it.

A problem with this state of the art procedure is however that the code may still be traceable within the material. By obtaining the same material from different sources, different copies will have different identification codes. It is then relatively easy to find the areas where the identification codes are hidden, especially on digitally distributed material, by plain comparison of the two copies. Theoretically, since the copies are identical, apart from the identification code, subtracting the signal of one copy from the other will result in a signal comprising only the two different identification codes. It is then possible to remove or obscure the relevant

sections, making the identification codes unobtainable and thereby removing the possibility of tracking illegal copies.

US 5,394,274 discloses a system for preventing unauthorised copying of audio or video recordings by (1) processing the recorded material so as to identify the protected material in a manner that does not audibly distort the program material, and (2) processing the recorded material by a second method that produces audible artifacts. Equipment capable of removing the audible artifacts while retaining the inaudible identification signal would be installed in audio digital tape recorders or video recorders so as to allow the equipment to be used for playback purposes while at the same time discouraging the unauthorised copying of audio, video or motion picture protected material. The proposed solution suffers inter alia from the drawback the need for special equipment to be installed for playback purposes. Furthermore, it does not deal with, nor solve, the problem of preventing detection of identification markings or the like encoded into digitally recorded data.

Object of the invention

It is a general object of the present invention to provide a method and an apparatus for improving traceability of the source of illegally copied and distributed media, such as video and audio recordings. More specifically, an object of the invention is to overcome the known deficiencies of the prior art techniques regarding identity code marking of digital recorded data streams, by providing the material with an identity code which is not easily found by simple comparison between two copies of the same material having different identity codes.

Summary of the invention

The above mentioned objects of the present invention are fulfilled by a method and an apparatus for implementing an identification code together with the data of a data stream, and to actively introduce a disturbance signal into the data stream, obscuring the presence of the identification code. In a preferred embodiment the disturbance signal is true random noise at a level below the cognitive threshold of a viewer or listener of the material that is represented by the data stream. The magnitude of the noise is on average the same as the changes in the data introduced by the insertion of the identity code.

Since the noise has true random behaviour, subtraction of one copy from another will not lead to any decrease in noise level. Hence, such a comparison will not lead to the uncovering of the identity codes. The inventive apparatus and method is preferably used for recording audio or video material on digital recording media, including optical means such as DVD and CD as well as magnetic tape

recording media, but is also useable for analog recordings. The invention is particularly suitable for marking video data streams transmitted to a video-on-demand user.

According to a first aspect, the invention relates to a data stream preparing apparatus for implementing an identification code together with the data of such a data stream, comprising: an input for a data stream; means for actively introducing a disturbance signal into said data stream; means for inserting a predetermined identification code into said data stream; and an output for the data stream including the inserted code and disturbance signal. A data stream transformer, connectable to said data stream input, preferably has a control signal input connected to a signing key transformer, and to a random disturbance signal source.

According to a second aspect, the invention relates to a method for marking a data stream, comprising the steps of: inputting a data stream into a data stream transformer of a marking apparatus; inputting a predetermined identification code control signal into a control signal input of the data stream transformer; inputting a random disturbance signal into said control signal input; inserting a predetermined identity code by transforming said data stream dependent on the signals input in said control signal input; outputting the transformed data stream from the marking apparatus.

According to a third aspect, the invention relates to a data stream transformer for implementing an identification code together with the data of an input data stream, comprising: a data stream input; a control signal input connectable both to a signing key transformer, and to a random disturbance signal source; transforming means, for transforming an input data stream dependent on an input control signal; and a data stream output.

According to a fourth aspect, the invention relates to a system for identification marking of a data stream, the system comprising a control signal, and a data preparing apparatus for implementing an identification code together with the data of a data stream dependent on such a control signal, the apparatus comprising: a data stream input; a control signal input; transforming means, for transforming an input data stream dependent on an input control signal; a data stream output, said control signal comprising a predetermined identification code, and a random disturbance signal.

Brief description of the drawings

The invention is described in detail below with reference to the accompanying drawings of which:

figure 1 is a block diagram of the procedure for signing a data stream, according to an embodiment of the inventive method;

figure 2 is a schematic illustration of one embodiment of the inventive apparatus.

figure 3 is a schematic illustration of another embodiment of the inventive apparatus.

Detailed description of preferred embodiments

The present invention refers to identity marking of data streams representing recorded audio or video signals, such as music or movies. Numerous ways of introducing an identity code into an audio or video recording have been proposed, such that the identity code is inconceivable for the viewer or listener of the material, such as the aforementioned patent US 5,613,004. The identity code as such does not require a lot of bandwidth. Less than 100 bytes of code are enough to guarantee a uniquely coded copy for each person on the planet. The realisation of the identity code can be performed in many ways. For video, e.g., two adjacent pixels can be given an increased and decreased luminance amplitude respectively, still maintaining the correct average luminance. Performed correctly, such an identity code will not be conceivable by the viewer of the video material. For audio recordings the identity code can be realised by various amplitude changes or even by frequency or phase changes. The code is repeated on several, or preferably all frames of audio or video, making it possible to find the source identity using only a portion of the recording on an illegal copy. It is also possible to encode the identity code in the data stream, e.g. video, in a part of said stream that is not even devised to be presented to the viewer/listener.

However, the invention is not directly focused on the means or techniques for introducing the identity codes into the data streams, but is intended to be useable together with any of such state of the art means and methods for marking media recordings. The purpose of the invention is to make it much more difficult to find the identity code of a copy of a recording by a simple comparison with another copy with a recording of the same material but with another identity code. The reason why the identity codes can be found by this comparison is that apart from the identity code the material, or data streams representing the material, is more or less the same. Evidently, the problem is more severe for digital recordings, since in that case the data streams are in fact identical. According to the present invention, the way of overcoming the problem that the identity codes can be easily found by comparison of different copies is to prepare each copy of a certain recording to be unique, even without the identity code. Furthermore, the difference between two copies shall not be conceivable by a viewer or listener of the material from two different copies. The proposed way of achieving this is to actively introduce a disturbance signal into the data stream of the recording. This disturbance signal

must be unique to the extent that two copies of the same recording must not have the same disturbance signal.

In a preferred embodiment of the present invention the disturbance signal is achieved by a true random noise generator, also called a Hardware Random Number Generator. As previously mentioned, the level of the noise must not be such that it is noticeable by a viewer of the material when playing the noise impeded copy. The disturbance signal may, as previously mentioned for the identification code, also be introduced in parts of the data stream that do not represent information that is to be presented to the viewer/listener. By using true random noise, the disturbance signal, however small, will be completely unique for each copy. A difference between the disturbance signal and the identity code, which also preferably is unique for every copy or group of copies, is that the pattern of the disturbance signal is unknown although it is actively introduced. The disturbance signal characterised by true random noise can not be reduced by recording by simple comparison between two copies. Subtraction or addition of the signals from two different copies will give the same result, namely a doubled noise level. Subsequent averaging can of course be performed but the resulting level of noise will be the same as for any of the two compared copies.

The chances that a variation in a data stream at a certain pixel, or time and frequency of the data stream, should occur both due to the disturbance signal and to a part of the identity code, are slight. Even though this chance exists, someone who is trying to trace the source of the illegal copy, having knowledge of where the identity code is situated, will easily find it over an extended portion of the data stream, due to redundancy of the repeated identity code. The same type of redundancy will actually leave traces of both of the used copies for making an illegal copy by the previously described subtraction method. Trying to get rid of the identity code by reducing all the noise of a copy will lead to an illegal copy with a deteriorated quality, clearly conceivable by the viewer or listener. Obviously, such a copy does not pose the same threat to the copyright holder as a perfect copy of digital material, as can be achieved from noise free digital recording media.

The identification code may be constructed by using a variety of different methods as previously mentioned. It would be an advantage if these methods be regularly changed as this would make the work more difficult for an attacker. These methods, including the identification codes themselves and all secret parameters used, should be kept secret by the copyright holder. As the bandwidth needed for noise injection is very limited, as compared to the bandwidth utilised by the material itself, the quality problem associated with the noise injection will be slight or diminutive. In one embodiment of the present invention a secret key stream cipher, or a Pseudo Random Number Generator, is used instead of a true random

noise generator to generate the disturbance signal. Since the number of identical copies to be individually signed and distributed are often counted in thousands, it is not necessary to use a true random number generator.

The inventive apparatus and method is applicable to the insertion of an identity code, in the form of a signature key, and a disturbance signal in data streams representing e.g. recorded music or speech, a picture or moving pictures, a computer or video game, or a computer program. With reference to the block diagram of Fig. 1, the procedure of the inventive method is first to take an unsigned data stream, such as a digital video recording, and second to add noise to the data stream. The data stream comprising noise is then marked by use of some appropriate method, as previously described. When marking the stream, a signing key is provided and used for performing a transformation in order to give this specific copy, or group of copies, a marking inside the data stream. The result is a data stream comprising both the key and noise. If the copyright holder at some point gets hold of an illegal copy of the data stream, such as a movie, the source of the copy is easily revealed, essentially by reversing the method of Fig. 1. In an alternative embodiment of the invention, the steps of adding noise and signing the stream are reversed, i.e. the stream is first signed, after which noise is added. In yet another embodiment, noise addition and signing transformation is achieved in one step.

With reference now to Fig. 2, an exemplified embodiment of the data stream preparing apparatus 1 according to the invention is shown. The apparatus 1 comprises a first input 2 for a data stream. A second input 3 is devised for input of noise. In a noise adder 4 comprised in the inventive apparatus 1, an input data stream from the first input 2 is added with noise from the second input 3. The apparatus 1 further has a third input 5 for a signing key. The signing key is preferably a code for the purchaser, or receiver, of the copy, but can also contain information on the distributor, the copying date, etc. A signing key transformer 6 in the apparatus 1 is devised to transform the input code by a secret procedure, in a manner well known in the art. A signing adder 7, comprised in the apparatus 1, is then useable for adding the transformed code into the noise impeded data stream, before outputting the signed data stream comprising noise through an output 8 of the apparatus 1.

Figure 3 illustrates an alternative embodiment of the apparatus 1 according to the invention. In this embodiment, the apparatus 1 comprises a first input 2 for a data stream. A second input 3 is devised for input of noise from a random disturbance signal source. Alternatively, the apparatus may comprise a noise generator, constituting the source of the random disturbance signal. The apparatus further has a third 5 input for a signing key. A signing key transformer 9 in the

apparatus 1 is devised to transform the input code by a secret procedure, in a manner well known in the art. The output of signing key transformer 9 is a control signal useable by a data stream transformer 10, connected to the signing key transformer 9 by a control signal input 11. The data stream transformer 10 has a data stream input 12, connectable to input 2, and a data stream output 13, connectable to output 8.

The data stream transformer 10 comprises data stream transforming means, devised to transform the data stream dependent on a control signal inserted through said control signal input 11. Furthermore, said second input 3 for noise is connected to said control signal input 11 of the data stream transformer 10. Hence, the data stream transformer will not be able to separate between predetermined control signals originating from the signing key transformer 9, and random noise originating from input 3. Consequently, in case the identification code is not known in advance, it will be nearly impossible to detect in a prepared data stream which alterations are caused by the identification code, and which are caused by noise.

A feature of the invention is that the introduced noise and ID marking are of the same kind, since they are introduced by the same mechanism, namely by transformer 10, and are applied to the same portion of the data stream. That is, if the data stream is to be marked e.g. by an identification code creating pixel value variations in the picture frames of the video signal, executed by the transformer 10, this is also how and where the noise is added. Furthermore, the noise added is of the same magnitude as the identification code, if a magnitude can be related to the implemented marking. Or to put it in other words: The disturbance effect of the data stream created by the identification code marking and the disturbance signal, i.e. noise, implementation is the same. The difference is that the ID marking, being carefully chosen and controlled, has a pattern representing the identification code, and preferably a redundancy, whereas the disturbance signal is random. The disturbance signal obscuring the marking makes the identification code very difficult to locate. By comparing two copies, it is theoretically possible to identify the differences between them. However, the differences will comprise not only the parts of the ID markings that differ, but also all the noise. The only way of being sure that the identification code is deleted is hence to completely remove the portion of the data stream where the identification code is encoded.

In an embodiment of the invention, the apparatus may be realised in hardware as an electronic circuit, or as a part of an ASIC, Application Specific Integrated Circuit. The inventive apparatus may also be realised in software, as a computer program product for use with a data processing and storage system, for carrying out the inventive steps. Also, the inventive apparatus according to Fig. 2 may of course be realised using both hardware and software elements, and may comprise a

disturbance signal generator, such as a random number generator, instead of having an input for noise.

After the introduction of the identity code and the disturbance signal the data stream is preferably recorded on a recording medium. In the digital case, such recording medium can be e.g. a Compact Disc, a DVD or a Mini Disc. Analog copies can be made on traditional magnetic tapes, for instance. Another suitable field of application for the present invention is video-on-demand (VOD) services. For such a service the copyright holder, or someone authorised by the copyright holder, transmits the data stream representing a movie, chosen by the user of the service, over the public telephone network or other transmission media, and the user is then able to watch the selected video in his or her home without having to go to a traditional video store. In order to prevent video-on-demand users to illegally copy and distribute copies of ordered movies the data stream preparing apparatus according to the present invention is preferably used to sign the material by inserting a suitable identification code, and to insert a suitable amount of noise for the purpose of hiding the sign. Any recording performed by the VOD-user will then contain both the sign and the obscuring noise.

The advantage of the proposed method and means is that an attacker will find plenty of discrepancies between different copies independent of how these copies are obtained. It would be difficult to correct all such discrepancies and the attacker may in no way feel confident that no source of the original material can not be traced. The level of protection could be increased by using the described method layered. Different distribution networks could be given different copies protected by the described method which in turn would be protected in the distribution process before reaching the end-customers. This will protect the original material if the attacker is able to obtain a master copy.

CLAIMS

1. A data stream preparing apparatus (1) for implementing an identification code together with the data of such a data stream, comprising:
- an input (2) for a data stream;
- means (4,10) for actively introducing a disturbance signal into said data stream;
- means (6,7,10) for inserting a predetermined identification code into said data stream; and
- an output (8) for the data stream including the inserted code and disturbance signal.

2. A data stream preparing apparatus (1) for implementing an identification code together with the data of such a data stream, comprising:
- a data stream input (2);
- a data stream transformer (10), connectable to said data stream input (2), the data stream transformer (10) having
- a control signal input (11) connected to
- a signing key transformer (9), and to
- a random disturbance signal source (2).

3. The data stream preparing apparatus as recited in claim 1 or 2, further comprising a disturbance signal generator.

4. The data stream preparing apparatus as recited in claim 1 or 2, further comprising an input (2) connectable to a disturbance signal generator.

5. The data stream preparing apparatus as recited in claim 3 or 4, wherein said disturbance signal generator comprises a true random noise generator.

6. The data stream preparing apparatus as recited in claim 3, 4 or 5, wherein said disturbance signal generator comprises a secret key stream cipher.

7. The data stream preparing apparatus as recited in claim 6, wherein such secret key stream cipher is a Pseudo Random Number Generator (PRNG).

8. The data stream preparing apparatus as recited in any of the previous claims, devised to introduce the code and the disturbance signal into an input data stream representing recorded music or speech.

9. The data stream preparing apparatus as recited in any of the claims 1 - 7, devised to introduce the code and the disturbance signal into an input data stream representing a picture.

10. The data stream preparing apparatus as recited in any of the claims 1 - 7, devised to introduce the code and the disturbance signal into an input data stream representing moving pictures.

11. The data stream preparing apparatus as recited in any of the claims 1 - 7, devised to introduce the code and the disturbance signal into an input data stream representing a computer game.

12. The data stream preparing apparatus as recited in any of the claims 1-7, devised to introduce the code and the disturbance signal into an input data stream representing a computer program.

13. The data stream preparing apparatus as recited in any of the claims 1 - 7, devised to introduce the code and the disturbance signal into an input data stream representing a video game.

14. The data stream preparing apparatus as recited in any of the previous claims, wherein the introduced disturbance signal is below the cognitive threshold of a viewer or listener of the material represented by the output data stream.

15. The data stream preparing apparatus as recited in any of the previous claims, devised to record the output data stream with the introduced identification code and disturbance signal on a Compact Disc (CD) recording medium.

16. The data stream preparing apparatus as recited in any of the previous claims, devised to record the output data stream with the introduced identification code and disturbance signal on a DVD recording medium.

17. The data stream preparing apparatus as recited in any of the previous claims, devised to record the output data stream with the introduced identification code and disturbance signal on a Mini Disc (MD) recording medium.

18. The data stream preparing apparatus as recited in any of the previous claims, devised to record the output data stream with the introduced identification code and

disturbance signal on a magnetic tape recording medium.

19. The data stream preparing apparatus as recited in any of the previous claims, devised to transmit the output data stream with the introduced identification code and disturbance signal to a video-on-demand service receiving device.

20. The data stream preparing apparatus as recited in any of the claims 8 – 13, wherein said data stream and said code comprises digital data.

21. The data stream preparing apparatus as recited in any of the claims 8 – 13, wherein said data stream and said code comprises analogue data.

22. The data stream preparing apparatus as recited in any of the previous claims, wherein said means for inserting a predetermined identification code is devised to alter amplitude values of predetermined portions of the material represented by the data stream, to a predetermined degree.

23. A method for marking a data stream, comprising the steps of:
- inputting a data stream into a marking apparatus (1);
- introducing a disturbance signal into the data stream;
- inserting an identity code into the data of the data stream; and
- outputting the data stream, including the inserted code and disturbance signal, from the marking apparatus.

24. A method for marking a data stream, comprising the steps of:
- inputting a data stream into a data stream transformer (10) of a marking apparatus (1);
- inputting a predetermined identification code control signal into a control signal input (11) of the data stream transformer;
- inputting a random disturbance signal into said control signal input (11);
- inserting a predetermined identity code by transforming said data stream dependent on the signals input in said control signal input (11);
- outputting the transformed data stream from the marking apparatus.

25. The method as recited in claim 23 or 24, further comprising the step of recording the output data stream on a recording medium.

26. The method as recited in claim 23 or 24, further comprising the step of transmitting the output data stream to a video-on-demand service receiving device.

27. The method as recited in any of the claims 23 – 26, wherein said disturbance signal is noise generated by a true random noise generator.

28. The method as recited in any of the claims 23 – 27, wherein said identity code is inserted by varying predetermined portions of the data to a predetermined degree.

29. The method as recited in any of the claims 23 – 28, wherein the inserted disturbance signal is below the cognitive threshold of a viewer or listener of the material represented by the output data stream, and where the amplitude of said disturbance signal on average is of the same magnitude as the amplitude of said identity code.

30. A method for marking a recording of a digital audio or video data stream with an identity code, comprising the steps of:
- inputting a data stream into a marking apparatus;
- inserting an identity code into the data stream by varying predetermined portions of the data stream to a predetermined degree, below the cognitive threshold of a listener or viewer of the audio or video material represented by the data stream;
- generating true random noise;
- adding the noise to said predetermined portions of the data stream at a level below the cognitive threshold of a listener or viewer of the audio or video material represented by the data stream;
- recording a copy of the input data stream with the inserted identity code and the added noise on a digital recording medium.

31. A computer program product comprising means for directing a data processing system to perform functions as recited in any of the claims 1 – 19, or means for directing a data processing system to perform the method steps as recited in any of the claims 20 – 28.

32. A data stream transformer (10) for implementing an identification code together with the data of an input data stream, comprising:
- a data stream input (12);
- a control signal input (11) connectable both to a signing key transformer (9), and to a random disturbance signal source (3);
- transforming means, for transforming an input data stream dependent on an input

control signal;
- a data stream output (13).

33. A system for identification marking of a data stream, the system comprising a control signal, and a data preparing apparatus (1) for implementing an identification code together with the data of a data stream dependent on such a control signal, the apparatus comprising:
- a data stream input (2,12);
- a control signal input (11);
- transforming means, for transforming an input data stream dependent on an input control signal;
- a data stream output (8,13), said control signal comprising a predetermined identification code, and a random disturbance signal.

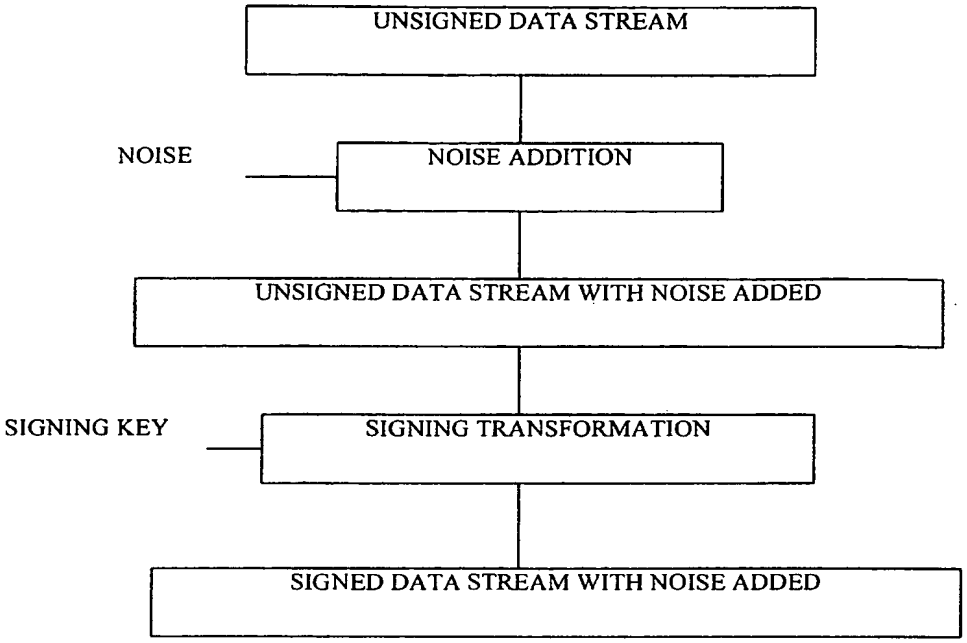

UNSIGNED DATA STREAM
NOISE
NOISE ADDITION
UNSIGNED DATA STREAM WITH NOISE ADDED
SIGNING KEY
SIGNING TRANSFORMATION
SIGNED DATA STREAM WITH NOISE ADDED

FIG. 1

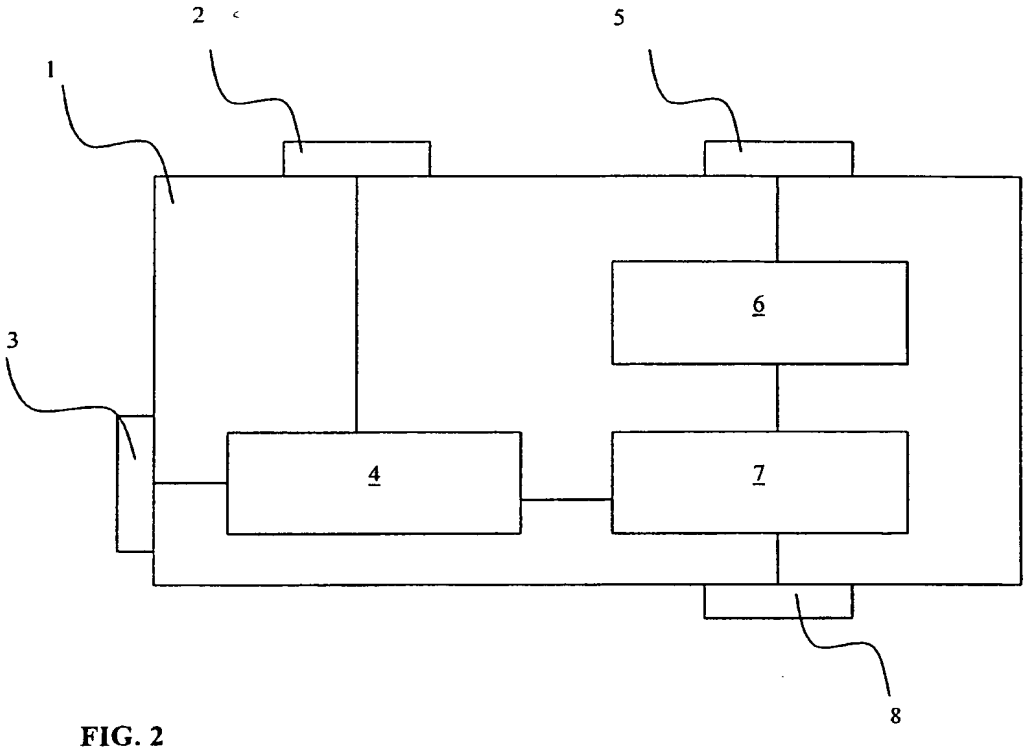


FIG. 2

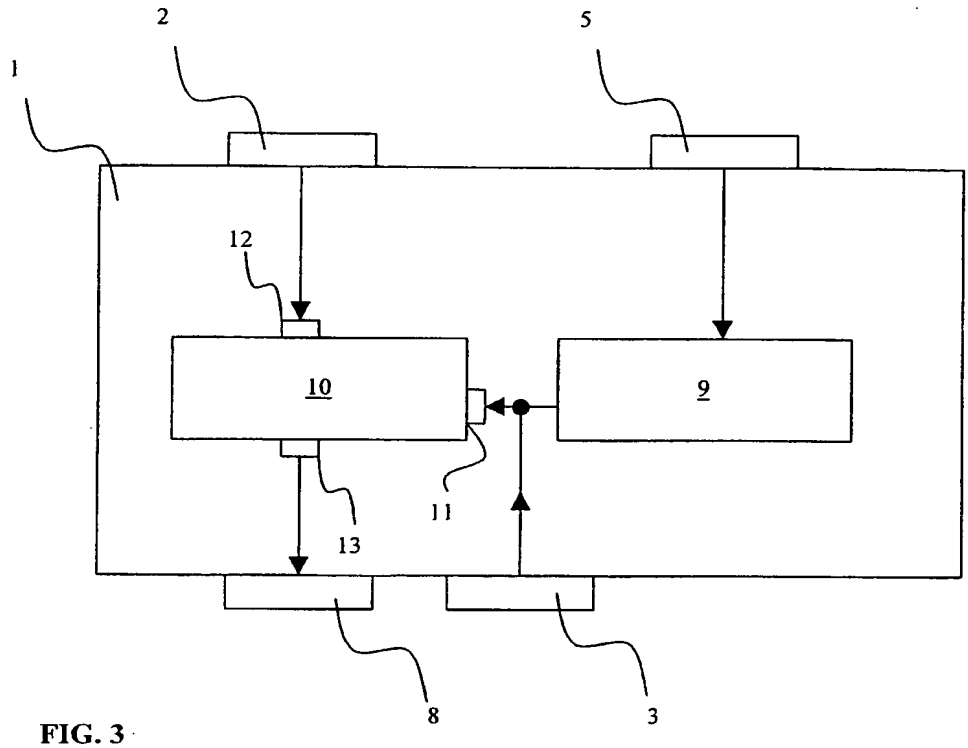


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/01835

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G11B 5/02, H04N 5/91
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G11B, G06F, H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5394274 A (KAHN), 28 February 1995 (28.02.95), column 4, line 1 - line 26; column 5, line 1 - column 6, line 7, figure 1, abstract --	1-33
A	EP 0589459 A1 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.), 30 March 1994 (30.03.94), column 2, line 42 - column 3, line 20, figure 1, abstract --	1-33
A	EP 0851679 A2 (NEC CORPORATION), 1 July 1998 (01.07.98), figure 1, abstract -- --------	1-33

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 February 2001	28. 02. 2001
Name and mailing address of the International Searching Authority European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel(+31-70)340-2040, Tx 31 651 epo nl, Fax(+31-70)340-3016	Authorized officer Ulrika Andersson /OGU Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SE 00/01835

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5394274 A	28/02/95	NONE	
EP 0589459 A1	30/03/94	DE 69312835 D,T	27/11/97
		JP 3010930 B	21/02/00
		JP 6103694 A	15/04/94
		US 5323244 A	21/06/94
EP 0851679 A2	01/07/98	CA 2225867 A	25/06/98
		JP 10191330 A	21/07/98